HAL open science

Distributed data fusion for situational awareness in critical infrastructures with link failures

Antonio Di Pietro, Stefano Panzieri, Andrea Gasparri

To cite this version:

Antonio Di Pietro, Stefano Panzieri, Andrea Gasparri. Distributed data fusion for situational awareness in critical infrastructures with link failures. 11th International Conference on Critical Infrastructure Protection (ICCIP), Mar 2017, Arlington, VA, United States. pp.99-117, 10.1007/978-3-319-70395-4_6 . hal-01819130

HAL Id: hal-01819130

https://inria.hal.science/hal-01819130v1

Submitted on 20 Jun 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Chapter 6

DISTRIBUTED DATA FUSION FOR SITUATIONAL AWARENESS IN CRITICAL INFRASTRUCTURES WITH LINK FAILURES

Antonio Di Pietro, Stefano Panzieri and Andrea Gasparri

Abstract This chapter presents a distributed data fusion algorithm for situational awareness in critical infrastructures whose link failures are based on the transferable belief model. The algorithm is applied to a case study involving a class of critical infrastructures that exchange the possible causes of the faults or threats that affect them. The algorithm is robust to communications link failures caused by natural disasters, cyber attacks or physical security breaches. Theoretical results show that algorithm convergence only requires the connectedness of the network topology over a certain time window, providing resilience in the face of temporary disruptions in the infrastructure communications layer.

Keywords: Distributed data fusion, information sharing, situational awareness

1. Introduction

Data fusion provides a means for combining pieces of information that come from diverse sources and sensors. Fusing this information can help bolster the security of critical infrastructure assets such as power grids and water distribution networks by providing improved situational awareness that can significantly enhance decision making. Critical infrastructure assets typically aggregate information coming from their sensors for their own use and do not share information about their operational states with other infrastructures. This is because disseminating sensitive information to other infrastructures can pose security problems, a topic that has been investigated by several researchers (see, e.g., [18]). However, the lack of information sharing about disaster mitigation procedures negatively affects disaster recovery, as in the case of the Sri Lanka tsunami of 2004 [13].

The U.S. Department of Homeland Security has spearheaded the creation of information sharing and analysis centers (ISACs) to facilitate information sharing efforts in the various critical infrastructure sectors. In fact, during real-time situations, aggregating information about the operations of multiple infrastructures can be very effective. For example, physical damage to a system can be assessed and then repaired in different ways depending on its cause (e.g., flooding due to heavy rainfall versus the opening of a valve by a computer virus). An accurate assessment of a situation obtained via data fusion can lead to successful incident response. Such an assessment requires all the relevant data to be available at the same time.

Ducourthial et al. [8] have proposed a distributed algorithm that implements data fusion in an unknown network topology. The algorithm computes the confidence of each node by combining all the data coming from its neighboring nodes using a discounted cautious operator and without relying on a central node for data collection. The algorithm converges in finite time for any initial configuration and any unknown network topology. However, the algorithm requires the network topology to become stable (i.e., nodes and links are fixed, and agents do not perform any dynamic observations) in order to reach convergence.

Considerable research has been conducted on applying data fusion techniques to enhance the security of critical infrastructure assets. Flammini et al. [9] have proposed a theoretical centralized framework for correlating events detected by a wireless sensor network in the context of critical infrastructure protection. This framework was leveraged in an early warning system that enhances decision making on combating security threats by collecting data from various sources. However, the centralized nature of this and other approaches – where all the data must be collected by a single node that performs data aggregation – reduces their robustness to node failure.

In contrast, this research advances the state of the art by eliminating the common assumption of a static network topology in order to accommodate scenarios where link failures may occur due to natural disasters, cyber attacks or physical security breaches. Specifically, a distributed data aggregation algorithm for situational awareness in critical infrastructures is presented, where the network topology that describes the communications layer is unknown and may change with time. The algorithm converges in finite time without requiring a stable network topology by engaging the cautious rule of combination [7] to aggregate data. This combination rule does not require the information sources to be independent or distinct and is, therefore, preferred to other rules (e.g., transferable belief model conjunctive rule [6] and Dempster combination rule [16] that lack robustness when information with equal credibility is combined several times). Because the cautious rule of combination is appropriate when all the sources are considered to be reliable, the convergence response is defined when all the sources are non-distinct and reliable. The effectiveness of the proposed algorithm is demonstrated using a case study involving several interconnected and interdependent critical infrastructures that are subjected to

physical failures. Addressing this challenging critical infrastructure protection scenario requires a novel distributed data fusion framework that can reduce the risk of cascading failures by dynamically sharing information between the infrastructures.

2. Preliminaries

The theory of evidence is a formalism for modeling imprecision and uncertainty without resorting to classical probability. This theory, introduced by Dempster [5] and Shafer [16], also referred to as the Dempster-Shafer theory, associates a number between zero and one to model the degree of confidence in a proposition based on partial (uncertain or imprecise) evidence.

Let $\Omega = \{\omega_1, ..., \omega_n\}$ be a finite set of possible values of a variable ω whose elements ω_i are assumed to be mutually exclusive. Let $\Gamma(\Omega) \triangleq 2^\Omega$ be the power set of Ω. The goal is to quantify the confidence of a proposition of the form: "The true value of ω is in γ" where $\gamma \in 2^\Omega$. The set Ω is referred to as the frame of discernment.

Basic Belief Assignment. A function $m : 2^\Omega \to [0, 1]$ is called a basic belief assignment (BBA) m if $\sum_{\gamma_a \in 2^\Omega} m(\gamma_a) = 1$ with $m(\emptyset) = 0$.

A basic belief assignment m can be equivalently represented by its associated commonality $q : 2^\Omega \to [0, 1]$ defined as:

$$q(\gamma_a) = \sum_{\gamma_b \supseteq \gamma_a} m(\gamma_b), \qquad \gamma_a \in 2^\Omega \tag{1}$$

Thus, for $\gamma_a \in 2^\Omega$, $m(\gamma_a)$ is the portion of the confidence that supports exactly γ_a. In other words, the true value of ω is in γ_a but, due to the lack of further information, it does not support any strict subset of γ_a.

A limitation of the Dempster-Shafer formulation is that the application of the Dempster combination rule [16] produces counterintuitive results when strong conflicts exist among the sources to be combined [19]. Smets [17] attempted to address this problem by proposing the transferable belief model (TBM), which relies on the concept of the basic belief assignment, but removes the assumption $m(\emptyset) = 0$. The removal of this assumption applies when the frame of reference is not exhaustive, so that it is reasonable to believe that another event, not modeled in the considered frame, will occur. This leads to the definition of the TBM conjunctive rule [6], which is more robust than the Dempster combination rule in the presence of conflicting evidence.

TBM Conjunctive Rule. The combination rule used in the transferable belief model removes the normalization constant in the Dempster combination rule. The new TBM conjunctive rule is defined as:

$$m_{ij}(\gamma_a) = \sum_{\gamma_b, \gamma_c; \gamma_b \cap \gamma_c = \gamma_a} m_i(\gamma_b) m_j(\gamma_c) \qquad \gamma_a \in 2^\Omega \tag{2}$$

The TBM conjunctive rule is associative and its use is appropriate when conflicts arise due to the low reliability of some of the data sources. However, this rule and the Dempster combination rule rely on the distinctness assumption of the sources; in other words, the information sources are independent. This limitation can be avoided using a combination rule with the idempotence property. Denoeux [7] defines an associative, commutative and idempotent operator called the cautious rule of combination, which is appropriate when all the sources are considered to be reliable. This rule does not require the assumption of independence.

Weight Function. Let m be a generic basic belief assignment. Then, the weight function $w : 2^{\Omega} \setminus \Omega \rightarrow \mathbb{R}^{+}$ is defined as:

$$w(\gamma_a) = \prod_{\gamma_b \supseteq \gamma_a} q(\gamma_b)^{(-1)^{|\gamma_b|-|\gamma_a|+1}} \qquad \forall \gamma_a \in 2^{\Omega} \setminus \Omega \tag{3}$$

$$= \begin{cases} \dfrac{\prod_{\gamma_b \supseteq \gamma_a, |\gamma_b| \notin 2\mathbb{N}} q(\gamma_b)}{\prod_{\gamma_b \supseteq \gamma_a, |\gamma_b| \in 2\mathbb{N}} q(\gamma_b)} & \text{if } |\gamma_a| \in 2\mathbb{N} \\ \\ \dfrac{\prod_{\gamma_b \supseteq \gamma_a, |\gamma_b| \in 2\mathbb{N}} q(\gamma_b)}{\prod_{\gamma_b \supseteq \gamma_a, |\gamma_b| \notin 2\mathbb{N}} q(\gamma_b)} & \text{otherwise} \end{cases}$$

Cautious Rule of Combination. Let m_i and m_j be two generic basic belief assignments in the transferable belief model with weight functions w_i and w_j, respectively. Then, their combination using the cautious conjunctive rule, denoted by $w_{i \ominus j} = w_i \ominus w_j$, is defined by the weight function:

$$w_{i \ominus j}(\gamma_a) = w_i(\gamma_a) \ominus w_j(\gamma_a) = \min(w_i(\gamma_a), w_j(\gamma_a)) \qquad \forall\, \gamma_a \in 2^{\Omega} \setminus \Omega \tag{4}$$

The proposed data aggregation technique works with the weight function w, which is obtained from masses using the commonality function q that is derived from the initial set of basic belief assignments. The next two sections demonstrate how these functions are generated from an initial set of basic belief assignments and are used to test the convergence of the algorithm.

3. Distributed Data Fusion

Consider a network described by an undirected graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}(t)\}$ where $\mathcal{V} = \{v_i : i = 1, .., N\}$ is a set of nodes (agents) and $\mathcal{E}(t) = \{e_{ij}(t) = (v_i, v_j)\}$ is a set of edges that represent the available point-to-point communications channels. The term t_k denotes the instant when the kth communication occurs in the network.

Four assumptions are made about the network of agents: (i) the network is described by a connected undirected graph; (ii) every node produces a local basic belief assignment expressed as a weight function called the direct con-

Algorithm 1 : Gossip algorithm.

$t = 0,\ s_i(0) = C_i(0)\ \ \forall\ i \in 1, ..., N$
$s_i(t_{stop})\ \ \forall\ i \in 1, ..., N$
while stop_condition == False **do**
  Select an edge e_{ij} in $\mathcal{E}(t)$ according to $\mathfrak{e}$
  Update the state of the selected agents according to $\mathcal{R}$
  $s_i(t+1) = s_i(t) \ominus s_j(t)$
  $s_i(t+1) = s_i(t) \ominus s_j(t)$
  $t = t + 1$
end while

fidence; (iii) agent communications are asynchronous – at every time instant t_k only one pair of agents (i, j) interact; and (iv) each agent i can handle the storage of the current direct confidence and the edge confidence computed via aggregation with a node v_j such that $(v_i, v_j) \in \mathcal{E}(t)$.

In the proposed framework, interactions between agents are modeled using a gossip algorithm [1]. An interaction is defined as a triplet $\{\mathcal{S}, \mathcal{R}, \mathfrak{e}\}$ for which the following conditions hold:

- $\mathcal{S} = \{s_1, ..., s_n\}$ is the set containing the local states $s_i \in \mathbb{R}^q$ of each agent i in the network such that $s_i(t) = (w_i(t, \gamma_1), .., w_i(t, \gamma_q))$ at time t with $q = |2^\Omega \setminus \Omega|$.

- $\mathcal{R}$ is the interaction rule based on the $\ominus$ operator that, for any two agents (i, j) with $e_{ij} \in \mathcal{E}(t)$, yields $\mathcal{R} : \mathbb{R}^q \times \mathbb{R}^q \to \mathbb{R}^q$ such that:

$$s_i(t) \ominus s_j(t) = (w_{i\ominus j}(t, \gamma_1), ..., w_{i\ominus j}(t, \gamma_q)) \tag{5}$$

- $\mathfrak{e}$ is the edge selection process, which specifies the edge $e_{ij} \in \mathcal{E}(t)$ that is selected at time t.

Algorithm 1 specifies the gossip algorithm used in this work. The term $C_i(0)$ in the algorithm denotes the initial direct confidence of agent i. Note that the algorithm does not require agents to have unique identifiers. In other words, agents are not required to know the identities of the neighbors with which they exchange information. This assumption is not cosmetic because security and confidentiality are common requirements in interdependent critical infrastructures [2].

Thus far, the gossip algorithm based on the $\mathcal{R}$ interaction rule has been presented. This update rule is similar to the min-consensus algorithm described by Cortes [3]. The major difference is that the proposed framework considers a gossip scheme and, thus, the interactions are asynchronous while Cortes [3] considers a consensus scheme where the interactions are synchronous.

Lemma 1: Consider a gossip algorithm $\{\mathcal{S}, \mathcal{R}, \mathfrak{e}\}$ over a time-varying graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}(t)\}$ with $\mathcal{S}$ and $\mathcal{R}$ as defined previously. Assume that each agent i at

time $t = 0$ provides an independent set of direct confidences described by the weight function values $s_i(0) = \{w_i(0, \gamma_a);\ \gamma_a \in 2^{\Omega} \setminus \Omega\}$ obtained from the basic belief assignments and commonality functions $m_i(0)$ and $q_i(0)$, respectively, via Equations (1) and (2). If $\mathfrak{e}$ is such that $\forall\, t$ there exists a $\Delta t \in \mathbb{R}$ where $\mathcal{G}(t, t + \Delta\, t)$ is connected, then there exists a time $t = \bar{t}$ such that $\forall\ t' > \bar{t},\ \ \forall\ \gamma_a \in 2^{\Omega} \setminus \Omega$ the following relation holds:

$$s(t') = s_1(0) \ominus s_2(0)\ \ominus \ldots \ominus s_n(0) \tag{6}$$

In other words, each agent i converges to the same weight function.

Proof: In order to prove the convergence of the algorithm to steady state, consider a generic network topology where $|V| = N$ is the number of agents (i.e., critical infrastructures). Consider the network at different time intervals $[t_0, t_0 + \Delta t_0]$, $[t_1, t_1 + \Delta t_1]$, ..., $[t_h, t_h + \Delta t_h]$ with $t_1 = t_0 + \Delta t_0 + 1$, $t_h = t_{h-1} + \Delta t_h + 1$. During each time interval Δt_i, the agents interact using the interaction rule $\mathcal{R}$ to form a connected graph. In particular, for any pair v_i and v_j such that $(v_i, v_j) \in \mathcal{E}(t)$ at time t, the cautious rule of combination is applied so that the two agents agree on the minimum of the weight function set values:

$$s_i(t) \ominus s_j(t) = (w_{1\ominus 2}(t, \gamma_1), .., w_{1\ominus 2}(t, \gamma_z)) \tag{7}$$

where $z = |2^{\Omega} \setminus \Omega|$.

Without any loss of generality, consider γ_a and assume that there exists an agent v_q such that $w_q(0, \gamma_a) = \overline{w}(0, \gamma_a) \leq w_m(0, \gamma_a)$ for $v_m \in\ \mathcal{V}$. Note that in each iteration, all the $w(t, \gamma_a)$ values with $\gamma_a \in 2^{\Omega} \setminus \Omega$ are compared between two agents to find the minimum value. For the sake of simplicity, consider a generic $w(t, \gamma_a)$ (the reasoning below will hold for any $w(t, \gamma_a)$). For each time interval Δt_k such that the graph $\mathcal{G}'(t_k + \Delta t_k)$ is connected, a particular edge selection policy is used that updates only one agent to $\overline{w}(t_k, \gamma_a)$. In addition, consider a partition of $P = \{U, W\}$ of $\mathcal{V}$ with $U, W \subseteq \mathcal{V},\ U\ \cap\ W = \emptyset,\ U\ \cup\ W = V$ where U contains the agents that have reached the $\overline{w}(t_k, \gamma_a)$ and $W = V \setminus U$ is the set of remaining agents. The worst-case scenario for the edge selection policy $\mathfrak{e}$, in terms of the number of interactions required to update the state of only one agent, is when it verifies that the connection between two agents $v_u \in U$ and $v_w \in W$ for which $e_{uv} = (v_u, v_w) \in \mathcal{E}'(t_k, t_k + \Delta t_k)$ occurs as the last interaction and the graph $\mathcal{G}'(t_k + \Delta t_k) = \{U \cup W,\ \mathcal{E}'(t_k, t_k + \Delta t_k)\}$ with $e_{uv} \in \mathcal{E}'(t_k, t_k + \Delta t_k)$ is connected.

Next, consider the worst-case topology of a network with N agents; this is the topology for which a larger number of updates is required to reach convergence when the worst-case edge selection policy is considered. Clearly, the worst-case scenario is the topology with the largest diameter d (i.e., line topology with $d = N - 1$).

Figure 1 shows the convergence to steady state at different time intervals for the worst-case network topology with $N = 5$, where the agent with $\overline{w}(t_i, \gamma_a)$ is placed on the extreme right so that the longest diameter is obtained. Note that

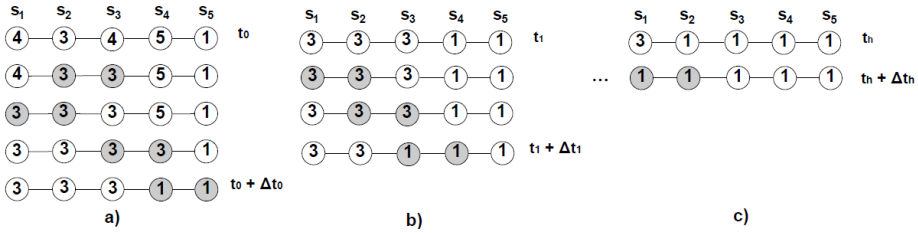


Figure 1. Steady-state convergence at different time intervals.

the number inside each circle represents the weight function set value $w_i(t_i, \gamma_a)$ of a generic set $\gamma_a \in 2^{\Omega} \setminus \Omega$ associated with agent i.

Now consider a time interval $[t_0, t_0 + \Delta t_0]$. Without any loss of generality, consider $|W| = N - 1$ and $|U| = 1$ at time t_0. At the exact time $t_0 + \Delta t_0$, two agents $v_u \in U$ and $v_w \in W$ communicate during the last iteration so that $|W| = N - 2$ and $|U| = 2$, which renders the graph $\mathcal{G}'(t_0 + \Delta t_0) = \{U \cup W,\ \mathcal{E}'(t_0, t_0 + \Delta t_0)\}$ connected.

Now consider a new time interval $[t_1, t_1 + \Delta t_1]$. At time t_1, $|W| = N - 2$ and $|U| = 2$. Now consider a new time interval $[t_h, t_h + \Delta t_h]$. At time t_h, $|W| = N-(h+1)$ and $|U| = h+1$. By iterating using the same reasoning for the edge selection policy, at the exact time $t_{N-1} + \Delta t_{N-1}$, two agents $v_u \in U$ and $v_w \in W$ communicate during the last iteration so that $|W| = 0$ and $|U| = N$, which renders the graph $\mathcal{G}'(t_{N-1}+\Delta t_{N-1}) = \{U \cup W,\ \mathcal{E}'(t_{N-1}, t_{N-1}+\Delta t_{N-1})\}$ connected. At this point, all the agents v_i for $i = 1..N$ have reached the same state $s(t') = \{\overline{w}(t', \gamma_a);\ \gamma_a \in 2^{\Omega} \setminus \Omega\}$. Therefore, $s(t')$ is at steady state in the multi-agent system. Since only one agent is updated during each time interval Δt_i, $d \cdot \Delta t_i$ (where d is the diameter of the network) is the number of time intervals $[t_i, t_i + \Delta t_i]$ after which all the nodes are updated. □

Lemma 2: Consider an edge selection policy $\mathfrak{e}$ such that $\forall\ t$ there exists a $\Delta t \in \mathbb{N}$ where $\mathcal{G}(t, t + \Delta\, t)$ is connected. If $\forall\ t$ there exists a time $M \in \mathbb{N}$: $\Delta\ t < M$, then any agent converges by $t = d \cdot M$ where d is the diameter of the network.

Proof: The proof follows directly from Lemma 1. In particular, recall that, in the worst-case scenario involving the topology, the network exhibits the largest diameter d so that $d = N - 1$ and $d \cdot \Delta t_i$ is the number of time intervals $[t_i, t_i + \Delta t_i]$ after which all the nodes are updated. Assuming that an upper bound M is available on the time required for the network to be connected during each time interval $[t_i, t_i + \Delta t_i]$, then the time required to update one agent is $t_i = M$. By iterating using the same reasoning, the process takes $t = d \cdot M$ to update all the agents. Therefore, the overall time required for the algorithm to converge in the worst-case scenario for the topology is linear with respect to the diameter of the network topology $\mathcal{G}$. □

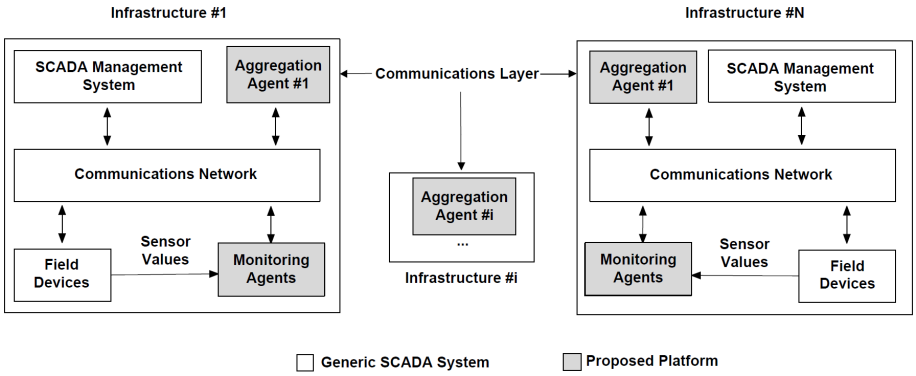


Figure 2. Communications framework between infrastructures in the case study.

4. Case Study

The case study involves a set of critical infrastructures in which the occurrence of certain conditions are monitored by a set of n agents. The infrastructures, which are geographically distributed, generically represent the infrastructure assets of a city. Each infrastructure is monitored by a SCADA system which includes: (i) a SCADA management system (e.g., human-machine interface and historian) located in a SCADA control center for monitoring and controlling field equipment; (ii) field devices (i.e., sensors, programmable logic controllers, remote terminal units and intelligent electronic devices) that acquire and transmit process parameter values and implement control actions; and (iii) a communications network that supports message exchange between field devices and the SCADA management system. Although critical infrastructures exhibit different kinds of dependencies, they generally do not share information. In contrast, this case study assumes that each infrastructure is able to produce information about the possible causes of faults in the infrastructure. This information, which is produced by monitoring agents deployed on the field devices, is exchanged among the agents (i.e., infrastructures).

The information shared among the infrastructures is provided by two kinds of agents as shown in Figure 2: (i) monitoring agents that acquire measurements from the field devices (physical events, cyber events and physical security events) and; (ii) aggregation agents that assist a SCADA management system by collecting the information from neighboring monitoring agents and distributing the information to peer agents in the other infrastructures. The resulting system is modeled as a multi-agent platform for distributed data aggregation in which each agent produces a basic belief assignment associated with the cause of a critical event that can affect the functionality of an infrastructure.

The monitoring agents, which detect physical and cyber events, are connected to the aggregation agents via the SCADA communications network of the associated infrastructure. Monitoring agents detect events by leveraging a security patrol, which is shared by the infrastructures to identify wireless

intruders that are proximal to the monitored infrastructures. A monitoring agent sends alarm condition notifications via wireless communications using the nearest infrastructure communications network. Every agent executes the algorithm presented in Section 3 in order to evaluate the direct confidence and to communicate with its neighboring nodes. Communications between the aggregation agents use virtual private network (VPN) links. Note that aggregation agents only aggregate information; their direct confidence values depend only on their neighboring nodes. The convergence of monitoring and aggregation agents occurs in finite time steps, providing the most credible cause(s) of a fault. According to Lemmas 1 and 2, algorithm convergence in finite time is ensured for any edge selection policy $\mathfrak{e}$ that produces a connected graph. This property is especially important in a disaster environment (such as the considered scenario), where communications paths between pairs of nodes may be unavailable.

Since the security patrol is mobile, its links with peer aggregation agents change over time. For simplicity, it is assumed that the security patrol is connected to only one aggregation agent during each time step – in any case, according to Lemma 1, a violation of this assumption does not affect the convergence of the algorithm.

The proposed approach is distributed because it can be implemented in a network without a central node. It differs from the centralized approaches that are typically employed in traditional SCADA system architectures. In a centralized approach, the SCADA management system gathers and correlates events and security information originating from field equipment in order to detect malicious activities that are perpetrated in a distributed manner – such a centralized node is able to produce more accurate information about the state of the monitored system. In contrast, the proposed approach is distributed because the SCADA management system nodes (manifested by aggregation agents) act as neutral nodes with initial basic belief assignments such that $m(\Omega) = 1$. These nodes provide valuable information when they perform aggregations in conjunction with other information agents.

4.1 Problem Formulation

The case study considers four interdependent critical infrastructures that can be affected by failures and/or threats. Each infrastructure is able to produce one or more basic belief assignments from physical, cyber and physical security events detected by the monitoring agents. The frame of discernment is $\Omega = \{a, b, c, d\}$ where a denotes a possible physical failure, b a possible cyber intrusion or attack, c a possible physical security threat and d a normal functioning level.

Figure 3 presents the case study scenario derived from [10], which involves a dam that feeds a hydroelectric power station that, in turn, feeds a power distribution substation through a transmission network (not modeled for simplicity). A base transceiver station (BTS) provides telecommunications services and receives electricity from the power distribution station. The dam provides

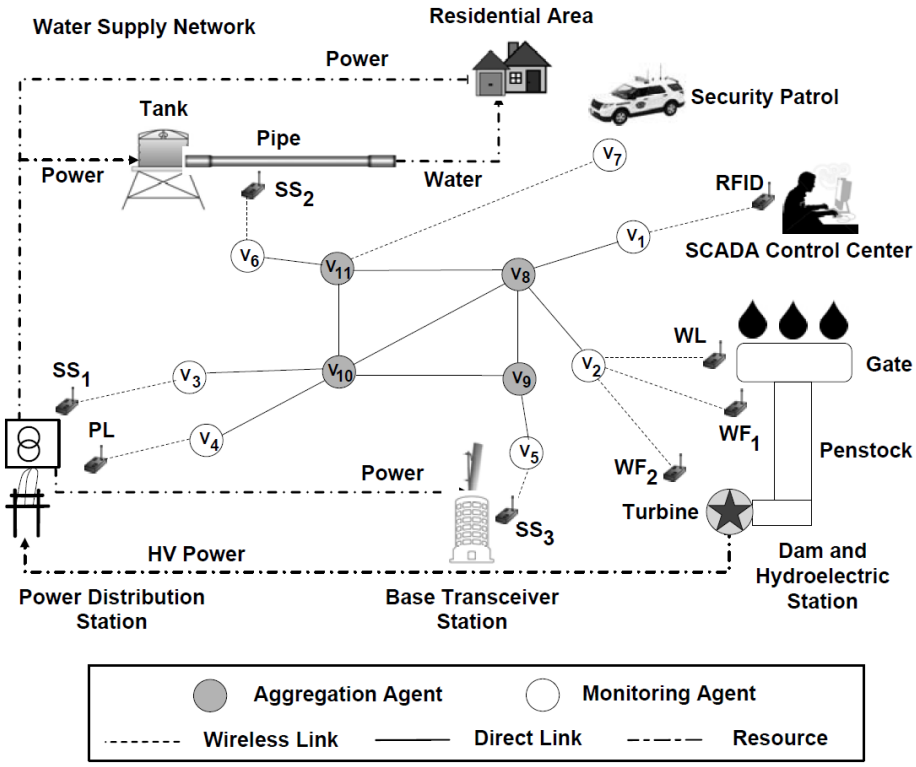


Figure 3. Case study scenario.

water to the hydroelectric power station through a gate that is remotely controlled to release basin water and activate the power plant turbine. The water supply network feeds the water pumps and automation devices, all of which receive electricity from the power distribution station. Infrastructure failures potentially cause societal and economic disruptions in the city district.

Table 1 shows the monitoring agents considered in each infrastructure. The following sections present practical methods that can be implemented by the agents to generate the relative basic belief assignments from sensor measurements. Also, the convergence of the algorithm starting with an initial set of basic belief assignments is demonstrated.

4.2 Dam and Hydroelectric Power Station

The dam and hydroelectric power station are controlled by a SCADA system that utilizes a wireless sensor network. Water fed to the hydroelectric power station is conveyed through pipes called penstocks. Agent v_1 is configured to monitor unauthorized physical access to the SCADA control room of the dam. In particular, the agent receives information wirelessly from a radio frequency identification (RFID) door sensor installed in the SCADA control room and

Table 1. Monitoring agents considered in each infrastructure.

Infrastructure	**Agents**
Dam and Hydroelectric Station	v_1, v_2
Power Distribution Station	v_3, v_4
Base Transceiver Station	v_5
Water Supply Network	v_6
Security Patrol	v_7

sends alerts about possible intrusions that could impact the proper functioning of the dam.

Table 2. Basic belief assignment generated by agent v_1.

A	$\mathbf{m_1(A)}$	
	Door Closed	**Door Open**
d	0.9	–
ac	–	0.3
bc	–	0.4
abc	–	0.2
Ω	0.1	0.1

When modeling the basic belief assignment of agent v_1, it is necessary to consider the possibility that an intruder with access to the SCADA control room may be able to launch a cyber attack (Table 2).

Agent v_2 periodically monitors the water flow rates and water levels measured by the sensors and uses them to check for security violations that could cause a turbine control malfunction. As explained in [10], two conditions hold in a generic dam under normal conditions: (C1) the difference between the water flow rates as measured by two water flow sensors located at the extremes of the penstock (WF_1 and WF_2 in the scenario) should disappear within about three seconds; and (C2) the variation in the water level in the basin of the dam (WL in the scenario) should be consistent with the variations in the incoming and outgoing water flows. Although the violation of each individual condition cannot be considered to be a consequence of a cyber attack, but rather a physical failure, violations of both conditions can increase the credibility of a cyber attack. In fact, a possible attack scenario involves compromises of the water flow sensors in order to hide changes in the water flow rates in the penstock. Thus, the basic belief assignment generated by agent v_2 combines the verification/violations of the two security conditions (Table 3).

Table 3. Basic belief assignment generated by agent v_2.

A	$\mathbf{m_2(A)}$			
	C1, C2	**¬C1, C2**	**C1, ¬C2**	**¬C1, ¬C2**
d	0.9	–	–	–
ab	–	–	0.2	0.3
ac	–	0.3	0.1	–
ad	–	0.1	0.5	–
bc	–	0.2	–	0.5
abc	–	0.1	–	–
Ω	0.1	0.3	0.2	0.2

4.3 Power Distribution Station

Earthquakes and hurricanes are known to have devastating effects on power distribution systems. Thus, reinforced concrete, fire- and explosion-resistant walls or barriers are installed between major pieces of equipment such as transformers, circuit breakers and regulators housed in power distribution facilities. Torrential rains caused by hurricanes can affect distribution systems more severely than generation and transmission systems. Floods caused by heavy rainfall can damage low-hanging lines in a power distribution system and cause power disruptions.

Agents v_3 and v_4 provide early warnings about possible physical faults induced by seismic events and floods, respectively. Agent v_3 obtains peak ground acceleration (PGA) data from a seismic sensor SS_1 installed in the substation building and estimates the credibility of a physical fault on the power distribution station based on the structural properties of the building. The building is assumed to have one story and to be a recent reinforced concrete construction. These properties are associated with a seismic vulnerability index $I_v = 0$ from a value range of –6 to 60. Agent v_3 transforms the peak ground acceleration of a seismic event to a microseismic intensity index I_{MCS} using the following equation for a building with the properties mentioned above [4]:

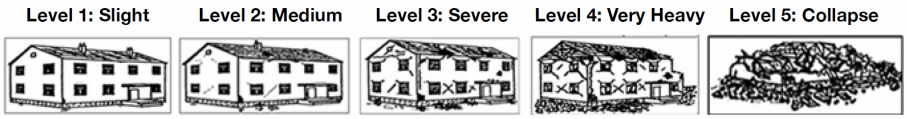
$$log(PGA) = 0.594 + 0.197 I_{MCS} \tag{8}$$

The following equations from [11] relate I_{MCS} and I_v to the mean damage d to the building (value range of 0 to 5) and the corresponding damage factor f_d (value range of 0 to 1):

$$d = 0.5 + 0.45(\arctan(0.55(I_{MCS} - 10.2 + 0.05 I_v)) \tag{9}$$

$$f_d = d^{1.75} \tag{10}$$

Based on these equations and the computed I_{MCS} and I_v values, agent v_3 can calculate the damage factor f_d (Figure 4) and estimate the credibility of a



Levels of Damage	0	1	2	3	4	5
Factor of Damage (f_d)	0	0.01	0.1	0.35	0.75	1

Figure 4. Expected damage [11, 15].

Table 4. Basic belief assignment generated by agents v_3 and v_5.

A	$\mathbf{m_3(A)}$					
	$\mathbf{f_d = 0}$	$\mathbf{f_d = 1}$	$\mathbf{f_d = 2}$	$\mathbf{f_d = 3}$	$\mathbf{f_d = 4}$	$\mathbf{f_d = 5}$
a	–	–	–	–	0.3	0.7
d	0.9	0.4	–	–	–	–
ab	–	0.3	0.4	0.5	0.6	0.2
ac	–	–	0.1	0.2	–	–
ad	–	–	0.2	–	–	–
Ω	0.1	0.3	0.3	0.3	0.1	0.1

physical fault affecting the power distribution station. Table 4 shows the basic belief assignment generated by agent v_3 based on the damage factor f_d.

Agent v_4 evaluates the rain precipitation in real time using a pluviometer sensor located in the substation; this data is used to assess the possible effects of flooding on the functionality of the substation. To accomplish this, a hot-spot analysis was conducted over a two-year period for a residential urban area. Linear regression analysis was then performed between the average frequency of disconnections at a specific electrical substation and the amount of rain precipitation in the area of the substation. Data relative to the rain precipitation was provided by a pluviometer installed near the substation.

The linear regression results in Figure 5 reveal a high correlation between the average frequency of disconnections and the amount of rain precipitation. This suggests that the amount of rain precipitation is a reliable predictor of the disconnection frequency and, therefore, provides a metric for specifying the basic belief assignment for agent v_4. Table 5 presents the credibility levels of physical faults in the substation of interest based on the daily quantity of rain precipitation denoted by Q (in mm).

4.4 Base Transceiver Station

A large number of base transceiver stations are installed in cities, often on the rooftops of buildings. This makes a base station vulnerable because an earthquake could damage the building housing the station, disrupting telecom-

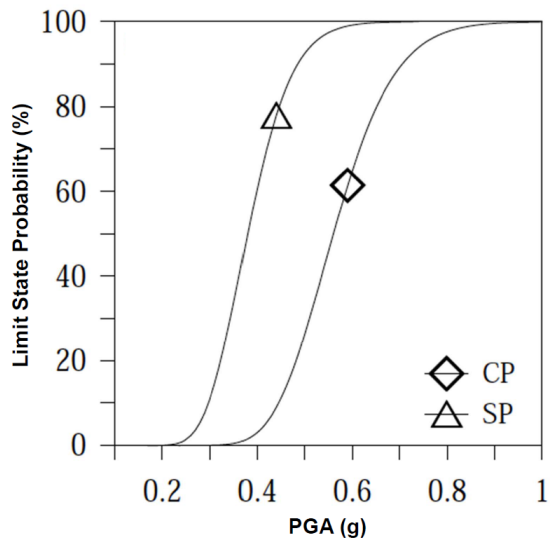


Figure 5. Correlation between the disconnection frequency and rain precipitation.

Table 5. Basic belief assignment generated by agent v_4.

A	$\mathbf{m_4(A)}$			
	$\mathbf{Q \leq 20}$	$\mathbf{20 < Q \leq 35}$	$\mathbf{35 < Q \leq 50}$	$\mathbf{Q > 50}$
a	–	–	–	0.6
d	0.9	0.3	–	–
ab	–	0.5	0.4	0.2
ac	–	–	0.1	–
ad	–	–	0.2	–
Ω	0.1	0.2	0.3	0.2

munications services in the area. Thus, agent v_5 could use the peak ground acceleration from the seismic sensor SS_2 installed in the building housing the base station to estimate the possible damage to the station based on the structural properties of the building. A building with the same structural properties as in Section 4.3, but with five stories (consistent with common base station installations) is considered. These properties can be associated with a seismic vulnerability index $I_v = 20$ according to Equations (9) and (10). Thus, agent v_5 is assigned the same basic belief assignment as agent v_3 in order to relate the damage level of the building to the occurrence of a physical failure to the base transceiver station.

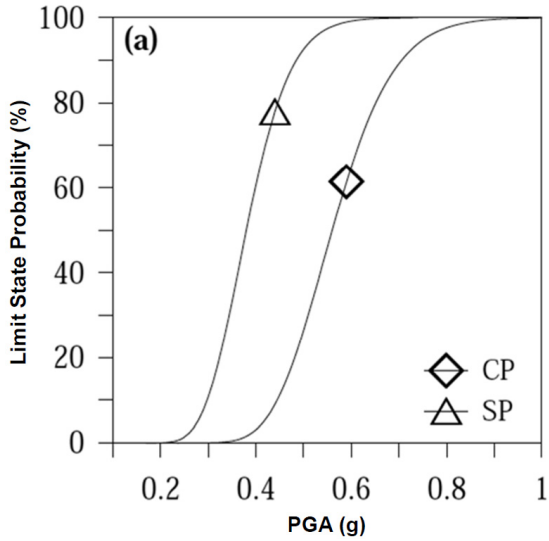


Figure 6. Fragility curve of a segmented pipeline [12].

4.5 Water Supply Network

Earthquakes are the most serious natural threat to a water supply network. They cause multiple types of damage to pipelines (e.g., longitudinal cracks, circumferential cracks and compression joint breaks) that result in severe water supply disruptions. To detect the effects of seismic events on the water supply network, agent v_6 acquires peak ground acceleration data from seismic sensor SS_3 installed in a pipeline that serves a residential area. The monitored segmented pipeline is assumed to have brittle iron pipes with bell-and-spigot joints, which is typical in water supply networks. The basic belief assignment generated by agent v_6 is determined by using the fragility curve for the specified pipeline as defined in [12] and diagrammed in Figure 6.

Table 6 shows the basic belief assignment generated by agent v_6. The value is proportional to the severity of the peak ground acceleration detected during an earthquake.

4.6 Security Patrol

The security patrol manifested by agent v_7 is based on the security vehicle prototype presented in [14]. The vehicle has equipment that detects wireless threats using the standard war-driving technique. The vehicle drives around a facility to collect and analyze wireless network traffic in order to detect potential intruders that are proximal to the facility. Predetermined security procedures are performed when threats are detected.

The security patrol vehicle can detect cyber and physical security threats. However, defining the basic belief assignment policy for this agent is application-

Table 6. Basic belief assignment generated by agent v_6.

A	$\mathbf{m_6(A)}$				
	PGA $\leq$ 0.2	**0.2 $<$ PGA $\leq$ 35**	**35 $<$ PGA $\leq$ 50**	**35 $<$ PGA $\leq$ 50**	**PGA $>$ 50**
a	–	–	–	0.3	0.7
b	–	–	–	–	–
d	0.9	0.5	0.1	–	–
ab	–	0.3	0.5	0.5	0.2
ac	–	–	0.2	0.1	–
bc	–	–	–	–	–
Ω	0.1	0.2	0.2	0.1	0.1

dependent because it requires a deep analysis of the environment monitored by the vehicle and the wireless traffic data. Indeed, to quantify the credibility of cyber and physical security threats in the form of a basic belief assignment, several properties should be considered, including the signal strength of the emitter and the number of packets collected. The stronger the signal, the more accurate the location of a potential intruder. Moreover, the greater the number of wireless packets collected, the more likely it is that a cyber attack would be discovered.

In this scenario, it is assumed that the security patrol can, at each time step, specify the credibility of cyber and physical security threats in terms of a basic belief assignment. This information is communicated periodically via a wireless connection to the aggregation agent of the infrastructure of interest.

4.7 Numerical Example

This section presents the results of executing the distributed data fusion algorithm for a specific set of basic belief assignments and a random topology generated at each time step. In order to establish algorithm convergence based on Lemma 1, the edge selection policy $\mathfrak{e}$ generated a random connected graph at each time step, where the edges between the agents may or may not have existed and the security patrol was connected to an aggregation agent that changed over time. This policy complies with the assumptions underlying the application of the algorithm in a disaster scenario where the communications network may undergo temporary or permanent disconnections.

Table 7 shows the set of basic belief assignments at time $t = 0$ corresponding to the network topology shown in Figure 3. It is assumed that the security patrol provides the same alarm conditions over time as agent m_7 in Table 7 when it monitors the water supply network. However, the security patrol provides no information (i.e., $m(\Omega) = 1$) when it monitors other infrastructures. The last row in Table 7 shows the convergent basic belief assignment $\overline{m}(\gamma_a)$ at time $\overline{t} = 106$, which was obtained using the weight function $\overline{w}(\gamma_a)$ as described in Section 2. The basic belief assignments $\overline{m}(\gamma_a)$ exhibit the highest credible values corresponding to the occurrence of a physical fault that affects the con-

Table 7. Example of initial basic belief assignments for agents v_1 to v_{11}.

BBA	$\emptyset$	**a**	**b**	**c**	**ab**	**ac**	**ad**	**bc**	**abc**	$\mathbf{\Omega}$
$m_1(0)$	–	–	–	–	–	–	–	–	–	1
$m_2(0)$	–	–	–	–	–	0.3	0.1	0.2	0.1	0.3
$m_3(0)$	–	–	–	–	0.5	0.2	–	–	–	0.3
$m_4(0)$	–	–	–	–	0.4	0.1	0.2	–	–	0.3
$m_5(0)$	–	–	–	–	0.5	0.2	–	–	–	0.3
$m_6(0)$	–	–	–	–	0.5	0.3	–	–	–	0.2
$m_7(0)$	–	–	–	–	–	–	–	0.3	0.4	0.3
$m_{8-11}(0)$	–	–	–	–	–	–	–	–	–	1
$\overline{m}(\overline{t})$	0.22	0.41	0.06	0.03	0.12	0.08	–	–	0.04	0.04

sidered infrastructures. It is worth noting that the same convergent basic belief assignments are obtained using a centralized approach where all the basic belief functions, expressed as weight functions, are aggregated using the cautious operator.

5. Conclusions

The proposed distributed data fusion algorithm based on the transferable belief model is designed to provide situational awareness in critical infrastructures with link failures. A key result is that the algorithm converges in finite time for any connected network topology when the cautious rule of combination is used for data aggregation. The application of the algorithm to a realistic scenario involving interdependent critical infrastructures demonstrates its utility as an information sharing methodology. Information sharing among infrastructures is extremely useful for decision making during emergency situations, enabling the understanding of the most credible causes of service degradation and the implementation of timely countermeasures.

Future research will focus on integrating additional agents to address a broader range of events that affect infrastructure assets (e.g., lightning and landslides).

References

[1] S. Boyd, A. Ghosh, B. Prabhakar and D. Shah, Randomized gossip algorithms, *IEEE Transactions on Information Theory*, vol. 52(6), pp. 2508–2530, 2006.

[2] F. Caldeira, M. Castrucci, M. Aubigny, D. Macone, E. Monteiro, F. Rente, P. Simoes and V. Suraci, Secure mediation gateway architecture enabling communications among critical infrastructures, *Proceedings of the Future Network and Mobile Summit*, 2010.

[3] J. Cortes, Finite-time convergent gradient flows with applications to network consensus, *Automatica*, vol. 42(11), pp. 1993–2000, 2006.

[4] L. Decanini and F. Mollaioli, Formulation of elastic earthquake input energy spectra, *Earthquake Engineering and Structural Dynamics*, vol. 27(12), pp. 1503–1522, 1998.

[5] A. Dempster, A generalization of Bayesian inference, *Journal of the Royal Statistical Society, Series B (Methodological)*, vol. 30(2), pp. 205–247, 1968.

[6] A. Dempster, Upper and lower probabilities induced by a multivalued mapping, in *Classic Works of the Dempster-Shafer Theory of Belief Functions*, R. Yager and L. Liu (Eds.), Springer, Berlin-Heidelberg, Germany, pp. 57–72, 2008.

[7] T. Denoeux, Conjunctive and disjunctive combination of belief functions induced by nondistinct bodies of evidence, *Artificial Intelligence*, vol. 172(2–3), pp. 234–264, 2008.

[8] B. Ducourthial, V. Cherfaoui and T. Denoeux, Self-stabilizing distributed data fusion, in *Stabilization, Safety and Security of Distributed Systems*, A. Richa and C. Scheideler (Eds.), Springer, Berlin, Germany, pp. 148–162, 2012.

[9] F. Flammini, A. Gaglione, N. Mazzocca, V. Moscato and C. Pragliola, Wireless sensor data fusion for critical infrastructure security, *Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems*, pp. 92–99, 2008.

[10] V. Formicola, A. Di Pietro, A. Alsubaie, S. D'Antonio and J. Marti, Assessing the impact of cyber attacks on wireless sensor nodes that monitor interdependent physical systems, in *Critical Infrastructure Protection VIII*, J. Butts and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 213–229, 2014.

[11] S. Lagomarsino and S. Giovinazzi, Macroseismic and mechanical models for the vulnerability and damage assessment of current buildings, *Bulletin of Earthquake Engineering*, vol. 4(4), pp. 415–443, 2006.

[12] G. Lanzano, E. Salzano, F. Santucci de Magistris and G. Fabbrocino, Vulnerability of pipelines subjected to permanent deformation due to geotechnical co-seismic effects, *Chemical Engineering Transactions*, vol. 32, pp. 415–420, 2013.

[13] C. Pathirage, D. Amaratunga, R. Haigh and D. Baldry, Knowledge sharing in disaster management strategies: Sri Lankan post-tsunami context, *Proceedings of the CIB World Building Congress*, pp. 2981–2993, 2007.

[14] I. Patterson, J. Nutaro, G. Allgood, T. Kuruganti and D. Fugate, Optimizing investments in cyber-security for critical infrastructure, *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, article 20, 2013.

[15] M. Pollino, G. Fattoruso, L. La Porta, A. Della Rocca and V. James, Collaborative open source geospatial tools and maps supporting response planning for disastrous earthquake events, *Future Internet*, vol. 4(2), pp. 451–468, 2012.

[16] G. Shafer, *A Mathematical Theory of Evidence*, Princeton University Press, Princeton, New Jersey, 1976.

[17] P. Smets, The combination of evidence in the transferable belief model, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 12(5), pp. 447–458, 1990.

[18] D. Sutton, J. Harrison, S. Bologna and V. Rosato, The contribution of NEISAS to EP3R, in *Critical Information Infrastructure Security*, S. Bologna, B. Hammerli, D. Gritzalis and S. Wolthusen (Eds.), Springer-Verlag, Berlin Heidelberg, Germany, pp. 175–186, 2013.

[19] L. Zadeh, On the Validity of Dempster's Rule of Combination of Evidence, Memorandum UCB/ERL-M, Electronics Research Laboratory, University of California, Berkeley, Berkeley, California, 1979.